

REMARKS

Applicants respectfully traverse and request reconsideration.

As a preliminary matter, Applicants' attorney wishes to thank Examiner Meislahn for the courtesies extended during the telephone conference of June 12, 2003. In response to these discussions, Applicants believe the above amendments and following remarks support allowance of all the claims.

As an additional matter, Claims 4, 14 and 28 have been included in their independent claims since these claims do not appear to be rejected and since they distinguish over the references of record in addition to the original language of the claims.

Claims 1-4, 6, 8-18, 20-24 and 26-30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis in view of Ellison. Applicants respectfully reassert the remarks made in previous Office Actions with respect to these references. In addition, as discussed during the telephone conference, Applicants' Claim 1, for example, is directed to among other things, selectable digital signature expiry data and a multi-client manager unit that provides on a per client basis, selectable digital signature expiry data. In addition, the claims require that a digital signature key pair update request has been received from a client unit and also that a new digital signature key pair is received from a client unit in response to the digital signature key pair update request. Multi-client management unit then associates the stored selected expiry data to create a new digital signature certificate containing the selected public key expiry data for the client that generated the digital signature key pair update request.

Lewis teaches an opposite. Applicants again reiterate that the Lewis reference teaches a completely different key replacement technique and also teaches that a key server accepts a key replacement command from a central public key controller which decides when to replace the active public key (Col. 7, lines 29-33). Hence, the client unit in Lewis does not generate keys

nor update key requests. As taught by Lewis, it is the key server that sends out a key replacement message containing the replacement key and a hash of its own replacement key. In contrast, Applicants claim that a multi-client manager unit determines whether digital signature key pair update request has been received and then receives the new digital signature key pair from the client. A multi manager unit then associates the selected expiry data with the new digital signature key pair to affect the transition from an old signature key pair to a new digital signature key pair. This is distinctly different from Lewis since the user node of Lewis does not determine whether digital signature key pair update is required, nor does it generate digital signature key pairs. As such, the claims are believed to be in condition for allowance.

As to the dependent claims, these claims add additional novel and non-obvious subject matter as pointed out in Applicants previous responses to Office Actions, including, but not limited to the Response filed November 8, 2002 incorporated herein by reference. Applicants also incorporate by reference the other remarks with respect to dependent claims.

Claims 5, 19, 25 and 27-29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis and Ellison and in view of Applicants admitted prior art. Claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Lewis and Ellison as applied to claim 1. Applicants respectfully reassert the remarks made above with respect to above claims 1, 14 and 21.

As to claim 5 for example, the Office Action takes official note that fixed length renewal periods are old and well known. The Office Action then concludes that it would have been obvious to set key update periods that are based on a fixed number of days and a percentage of a key's lifetime. Applicants respectfully submit that this is a mischaracterization of Applicants' claimed invention. Applicants note that conventional public key cryptographic systems typically

have a fixed default period that is the same for all clients on the system. The default period is fixed and it is typically not adjustable by a multi-client manager or certification authority as claimed. However, Applicants claim, *inter alia*, initiating, by a client unit, digital signature key pair update requests based on whether differences between a current date and a digital signature private key lifetime end date is less than an absolute predetermined period of time, and based on whether the difference between a current date and a digital signature private key lifetime end date is less than a predetermined percentage of a total duration of a digital signature private key lifetime when the digital signature private key lifetime was selectable on a per client basis through a multi-client manager unit. No such digital key pair update request or basis for such a request is taught or suggested in any of the references cited. It is Applicants' own disclosure which teaches such an invention which provides many advantages over conventional systems. Applicants respectfully request a showing of a teaching and references of such a digital signature key pair update request and the basis for initiating such a request as claimed.

Claims 1-4, 6, 8-18, 20-24 and 26-30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,003,014 (Lee et al) in view of Ellison. This is a new rejection of the claims.

Lee is directed to a method and apparatus for acquiring access using a smart card and in particular, attempts to solve a problem unrelated to Applicants claimed invention. For example, as Lee notes in the "Background of the Invention" section of his patent, Lee is directed to aiding transit passengers to gain access to transportation using smart cards by implementing an access system using an "open" stored value card system. The smart cards described in the Lee reference contain information representing, for example, money to allow the holder of the card to pay for the cost of transportation in public transportation settings. Accordingly, Applicants

respectfully submit that one of ordinary skill in the art would not be motivated to apply the teachings of Lee since it is directed to a completely different problem. Applicants claim a system and method for providing updated digital signature key pairs to a plurality of clients in a public key system.

In any event, for argument's sake, Applicants note that the Office Action has cited Columns 10 and 11 for allegedly teaching all of the claimed subject matter except that expiry data is selectable. Ellison has been cited for teaching setting public key validity periods according to risk management.

Applicants respectfully submit that teachings of the references do not render Applicants' claims obvious. For example, as to the independent claims, these claims require, among other things, that the system must update digital signature key pairs to affect a transition from an old digital signature key pair to a new digital signature key pair. The claims require that a digital signature key pair update request be generated and received. The Lee reference is silent as to a digital signature key pair update scheme and does not appear to teach or suggest, among other things, determining whether digital signature key pair update request has been received from a client unit or receiving a new digital signature key pair from a client unit in response to the digital signature key pair update request. Since the references are silent as to such digital signature key pair update request, these claims are in condition for allowance.

In addition, the Office Action attempts to equate the "issuing bank" with Applicants claimed "client unit." As noted above, Lee does not teach, among other things, that the issuing bank sends a digital signature key pair update request. Moreover, Lee merely describes a conventional certification authority hierarchy wherein the issuing bank serves as one certificate authority and a higher order certificate authority referred to as "the certificate authority"

generates an issuer certificate for the issuing bank. The issuing bank serves as a card issuer by generating a card certificate using a card public key pair and the issuing bank's secret key. (See Col. 10, lines 49-65). There is a discussion in the cited reference of how an issuing bank gets any updated key pairs or which entity determines whether a expiry period for digital signature key pair has occurred. Accordingly, the claims are in condition for allowance. In addition, the Lee reference is not directed to a digital signature key pair update mechanism as required by the claims. As noted in previous Office Action, the Ellison reference is also silent as to updating digital signature key pairs. Since none of the references teach the required claim limitations, Applicants respectfully submit that the claims are in condition for allowance.

Claims 5, 19, 25 and 27-29 stand rejected under 35 U.S.C. § 103(a) as being upatentable over Lewis and Ellison and further in view of Applicants' admitted prior art. Applicants respectfully reassert the remarks made above with respect to the Lee reference and as such these claims are also in condition for allowance. In addition, the references neither teach nor suggest the determination of a digital signature private key lifetime end date and creation date upon a user log in to the public key system. The references are silent as to such a teaching. In addition, none of the references or Applicants' prior art teaches that a client unit initiates a key pair update request based on whether the difference between a current date and a digital signature private key lifetime end date that was provided by a multi-client unit that provided selectable digital signature private key selection based upon the periods of times set forth in the claims. Accordingly, these claims are also believed to be in condition for allowance.

Applicants respectfully submit that the claims are in condition for allowance and a Notice of Allowance is respectfully solicited. The Examiner is invited to contact the below-listed

attorney if the Examiner believes that a conference would expedite the prosecution of the instant application.

Dated: June 12, 2003

Respectfully submitted,

By: 
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz
222 N. LaSalle Street, Suite 2600
Chicago, IL 60601
PH: (312) 609-7599
FAX: (312) 609-5005